Claims

1. A method for password enhancing, which method comprises the steps of entering a user password and irreversibly encrypting the user password.

2. A method according to claim 1, in which the encryption comprises a hash operation.

3. A method according to claim 1 or claim 2, in which the method comprises the additional step of using an encrypted first stored key (NEPKEY) to encrypt the irreversibly encrypted user password (HASH).

4. A method according to claim 3, in which the first stored key is encrypted by a public key encryption algorithm.

5. A method according to claim 3 or claim 4, in which the method comprises the additional step of decrypting an encrypted second stored key (UPEK) using the decrypted first stored key (NEPKEY).

6. A method according to claim 5, in which the second stored key is encrypted by a reversible algorithm.

7. A method according to claim 5 or claim 6, in which the result (HASH) of the irreversibly encrypted user password is encrypted using the second stored key (UPEK) as an encryption key.

8. A data access method comprising the steps of producing an enhanced password according to any one of claims 1 to 7,

comparing the enhanced password with a password associated with the data, and permitting access to the data only if the enhanced password and the data password correspond.

9. A computer program for carrying out the method of claim 8.

10. A carrier comprising a program according to claim 9.

11. A data communication system comprising an input device for generating a plurality of input signals available from a set of input signals and a character generator configured to receive an input signal and generate an output signal comprising a plurality of signals from the set of input signals in which the output signal is different from the signal input to the character generator.

12. A data communication system according to claim 11, in which the output signal is of a different length to the signal input to the character generator.

13. A data communication system according to claim 12, in which the output signal is longer than the signal input to the character generator.

14. A data communication system according to any one of claims 11 to 13, in which the system further comprises means for comparing the output signal with a stored password.

15. A data communication system according to claim 14, in which the comparison means further comprises means for

09763203.042201

outputting a signal dependent upon the correspondence of the output signal with the stored password.

16. A data communication system according to any one of claims 11 to 15, in which the input device comprises a keyboard.

17. A data communication system according to claim 16, in which the set of available input signals comprises all or part of the character set of the keyboard.

18. A data communication system according to any one of claims 11 to 17, in which the system comprises a first input and a second input in which the character generator receives signals from the first input and does not receive signals from the second input.

19. A data communication system according to claim 18, in which the first input is a local input device such as a keyboard or microphone and the second input is a remote based input device typically providing signals via a modem connection.

20. A data communication system according to claim 19, in which the input signal comprises or corresponds to one of the set of input signals.

21. A data communication system according to claim 20, in which the set of input signals comprises alphanumeric characters.

22. A digital computer comprising a data communication system according to any one of claims 11 to 21.

09763403.022301

~~23. A data communication method comprising receiving an input signal available from a set of input signals, generating an output signal comprising a plurality of signals from the set of available input signals, in which the output signal is different from the input signal.~~

~~24. A method according to claim 23, in which the method further comprises the step of repeating the operation for a plurality of input signals.~~

~~25. A method according to claim 23 or claim 24, in which the output signals vary in length one from the other.~~

AOD
A2

09763403 .022401